**מדריך יצירת משתמש בk8s**

בk8s יש מנגנון הרשאות בשם RBAC.  
איך מנגנון זה עובד על קצה המזלג? כמובן שבאמצעות אובייקטים.

הרשאות:  
Role – הרשאה לביצוע פעולות על אובייקטים בnamespace ספציפי.  
ClusterRole – הרשאה לביצוע פעולות על אובייקטים בכל הnamespaceים בcluster.

שיוך הרשאה:  
RoleBinding – שיוך הרשאה Role למשתמש.  
ClusterRoleBinding – שיוך הרשאה ClusterRole למשתמש.

משתמשים:  
serviceaccount – משתמש עבור תוכנה מסוימת שצריכה גישה לcluster. למשל Argo CD. ניתן ליצור אובייקט זה באמצעות kubectl.  
user account – משתמש עבור אדם בארגון. לא ניתן ליצור אובייקט כזה בcluster עצמו. יש צורך במנגנון הזדהות חיצוני כמו למשל: תעודות דיגיטליות, google account, משתמש דומייני וכו'.

* במדריך זה ניצור משתמש באמצעות תעודות דיגיטליות.

**יצירת משתמש לינוקסי**

useradd ron && cd /home/ron

passwd ron

**יצירת מפתח פרטי**

openssl genrsa -out ron.key 2048

**יצירת בקשה לתעודה דיגיטלית**

openssl req -new -key ron.key \

-out ron.csr \

-subj "/CN=ron"

* בעת היצירה של הבקשה אנחנו מחלצים את המפתח הציבורי מהמפתח הפרטי
* subj "/CN=ron” מגדיר מה השם של המשתמש

**חתימה של התעודה הדיגיטלית עם הCA של k8s**

openssl x509 -req -in ron.csr \

-CA /etc/kubernetes/pki/ca.crt \

-CAkey /etc/kubernetes/pki/ca.key \

-CAcreateserial \

-out ron.crt -days 500

* לוקח את הקובץ של הבקשה שיצרנו וחותם אותו באמצעות השרת CA של Kubernetes.

**העתקת קובץ config**

cp /root/.kube/config /home/ron/.kube/

chown ron:ron /home/ron/.kube/config

chown ron:ron /home/ron/.kube

* קובץ זה מכיל מידע אשר משתמש להזדהות מול api server כאשר אנחנו שולחים כל בקשה בkubectl.
* כרגע קובץ זה מכיל את ההרשאות של admin-user, בהמשך נמחק אותן.

**הוספת פרטי המשתמש לkubeconfig**

su – ron

kubectl config set-credentials ron --client-certificate=/home/ron/.certs/ron.crt --client-key=/home/ron/.certs/ron.key

kubectl config set-context ron-context --cluster=kubernetes --user=ron

vim /home/ron/.kube/config

change current-context value to “ron-context”

* כעת ברגע שנריץ פקודות של kubectl נתקל בבעיית הרשאות.

**יצירת namespace**

יש לבצע מהמשתמש root

kubectl create namespace ron-namespace

**יצירת Role**

vim role.yml

apiVersion: rbac.authorization.k8s.io/v1beta1

kind: Role

metadata:

name: ron-role

namespace: ron-namespace

rules:

- apiGroups: [""]

resources: [ "\*" ]

verbs: [ "\*" ]

kubectl apply -f role.yml

**יצירת RoleBinding**

Vim rolebinding.yml

apiVersion: rbac.authorization.k8s.io/v1

kind: RoleBinding

metadata:

name: ron-rolebinding

namespace: ron-namespace

subjects:

- kind: User

name: ron

apiGroup: rbac.authorization.k8s.io

roleRef:

kind: Role

name: ron-role

apiGroup: rbac.authorization.k8s.io

kubectl apply -f rolebinding.yml

**מעבר לnamesapce של המשתמש**

kubectl config set-context --current --namespace=ron-namespace

* כעת נוכל לבצע כל פקודה בnamespace שלנו